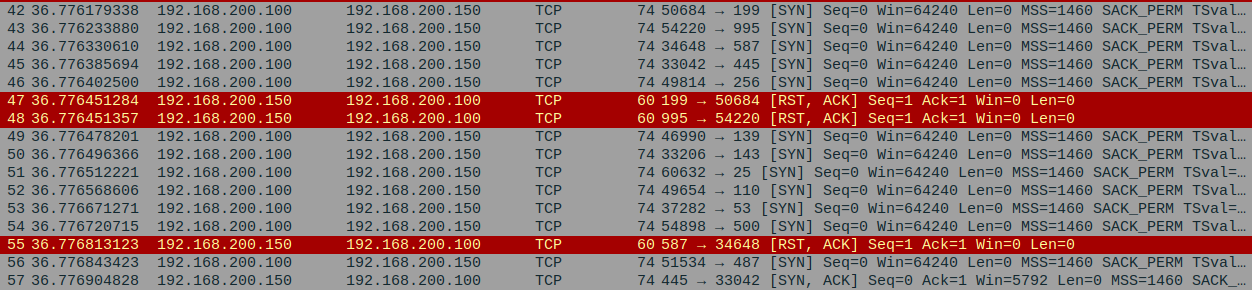
**Traccia:**

Per l’esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con *Wireshark*. Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

* Identificare eventuali IOC, ovvero evidenze di attacchi in corso;
* In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati;
* Consigliate un’azione per ridurre gli impatti dell’attacco.

Prima di andare a svolgere l’esercizio, scarichiamo l’allegato (cartella compressa), estraiamo il file e inseriamolo nella cartella condivisa che abbiamo creato in collegamento con la macchina virtuale Kali. Una volta aperto il file su quest’ultima si aprirà direttamente la schermata di **Wireshark**; un software di analisi di rete open-source ampiamente utilizzato per *monitorare e analizzare il traffico di rete in tempo reale*. È uno strumento potente che consente agli utenti di catturare e visualizzare i pacchetti di dati che vengono scambiati su una rete.



Già ad una prima analisi possiamo notare che vi sono un numero elevato di richieste **TCP [SYN]**, su porte sempre diverse, che partono dall’indirizzo IP **192.168.200.100** verso l’indirizzo IP **192.168.200.150.** Questo permette di rispondere alle prime due domande del quesito, ovvero:

1. Vi è un’evidenza di attacco in corso (**IOC**, indicatore di compromissione) viste le ripetute richieste TCP;
2. Con ogni probabilità la macchina *target* è rappresentata dall’IP 192.168.200.150, attaccata dall’host con IP 192.168.200.100, ipotesi avvalorata dal fatto che per alcune righe della cattura vediamo risposte positive del target **[SYN+ACK]** (riga 57) ad indicare che la porta è aperta. Per altre, invece, notiamo la risposta **[RST+ACK]** ad indicare che la porta è chiusa.

Da qui potremmo ipotizzare alcune contromisure da adottare, a livello di Firewall, per ridurre gli impatti di un attacco di questo tipo.

Infatti, modificando le regole del Firewall si potrebbe ad esempio:

* *limitare il numero massimo* di connessioni TCP in ingresso da un singolo indirizzo IP, per ridurre l'impatto di un attacco che cerca di sovraccaricare le risorse del server con un elevato numero di connessioni;
* *filtrare gli indirizzi IP*, così da creare una lista nera che blocchi i potenziali IP dannosi;
* *monitorare attentamente il traffico di rete* in tempo reale per identificare eventuali anomalie o comportamenti sospetti che potrebbero indicare un attacco in corso;
* *creare un piano di risposta agli incidenti* per gestire rapidamente e in modo efficace gli attacchi TCP. Questo piano dovrebbe includere procedure per isolare il traffico dannoso, notificare il personale di sicurezza e mitigare l'impatto dell'attacco sulle operazioni di rete.

Implementare queste **contromisure** può contribuire a proteggere efficacemente la rete e i servizi dai tentativi di attacco TCP, garantendo al contempo che il traffico legittimo possa fluire senza interruzioni. Ovviamente è fondamentale mantenerle sempre *aggiornate e adattarle* alle nuove minacce e agli attacchi emergenti.